Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33	(James near Vogt).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L2	69	(Robert near Hasbun).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L3	13	(John near Brizek).in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L4	106	L1 or L2 or L3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L5	5126	(authenticat$3 or password or passcode or keycode) near3 valid	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L6	84627	flash adj (memory or array)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L7	688	write adj2 state adj2 (machine or manager$2)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L8	28	L5 and L6 and L7	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L9	67688	(unauthoriz$4 or protect$3 or hidden or lock$4) near2 (area or section)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L10	13	L6 and L9 and L7	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27

L11	67688	(unauthoriz$4 or protect$3 or hidden or lock$4) near2 (area or section)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L12	688	write adj2 state adj2 (machine or manager$2)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L13	84627	flash adj (memory or array)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L14	67688	(unauthoriz$4 or protect$3 or hidden or lock$4) near2 (area or section)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L15	13	L13 and L14 and L12	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L16	1023	L13 and L14	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L17	421	invalid adj2 password	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L18	1023	L13 and L14	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L19	1	L17 and L18	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27
L20	196	bad near password$2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:27

L21	196	bad near password$2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:28
L22	3	L18 and L21	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:28
L23	0	((((authenticat$3 or password or passcode or keycode) near3 valid) and (flash adj (memory or array))) and ((unauthoriz$4 or protect$3 or hidden or lock$4) near2 (area or section))) and (invalid adj2 password)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:29

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+authentication, +password, +permit, +counter, +limit SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **authentication password permit counter limit**

Found **59** of **164,603**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 59

Result page: **1** 2 3 next

Relevance scale □ ▄ ▄ ▄ ■

1 Strong password-only authenticated key exchange

David P. Jablon

October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

2 A taxonomy of computer program security flaws

Carl E. Landwehr, Alan R. Bull, John P. McDermott, William S. Choi

September 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 3

Publisher: ACM Press

Full text available: pdf(3.81 MB) Additional Information: full citation, abstract, references, citings, index terms, review

An organized record of actual flaws can be useful to computer system designers, programmers, analysts, administrators, and users. This survey provides a taxonomy for computer program security flaws, with an Appendix that documents 50 actual security flaws. These flaws have all been described previously in the open literature, but in widely separated places. For those new to the field of computer security, they provide a good introduction to the characteristics of security flaws and how they ...

Keywords: error/defect classification, security flaw, taxonomy

3 Limitations of the Kerberos authentication system

S. M. Bellovin, M. Merritt

October 1990 **ACM SIGCOMM Computer Communication Review**, Volume 20 Issue 5

Publisher: ACM Press

Full text available: pdf(1.12 MB) Additional Information: full citation, abstract, citings, index terms

The Kerberos authentication system, a part of MIT's Project Athena, has been adopted by other organizations. Despite Kerberos's many strengths, it has a number of limitations and some weaknesses. Some are due to specifics of the MIT environment; others represent deficiencies in the protocol design. We discuss a number of such problems, and present solutions to some of them. We also demonstrate how special-purpose cryptographic hardware may be needed in some cases.

4 Protection and the control of information sharing in multics
Jerome H. Saltzer
July 1974 **Communications of the ACM**, Volume 17 Issue 7
Publisher: ACM Press
Full text available: pdf(1.75 MB) Additional Information: full citation, abstract, references, citings, index terms

The design of mechanisms to control the sharing of information in the Multics system is described. Five design principles help provide insight into the tradeoffs among different possible designs. The key mechanisms described include access control lists, hierarchical control of access specifications, identification and authentication of users, and primary memory protection. The paper ends with a discussion of several known weaknesses in the current protection mechanism design.

Keywords: Multics, access control, authentication, computer utilities, descriptors, privacy, proprietary programs, protected subsystems, protection, security, time-sharing systems, virtual memory

5 Authentication in office system internetworks
Jay E. Israel, Theodore A. Linden
July 1983 **ACM Transactions on Information Systems (TOIS)**, Volume 1 Issue 3
Publisher: ACM Press
Full text available: pdf(1.28 MB) Additional Information: full citation, references, index terms

6 The GUIDE: (graphical user interface designed for education)
Mark Resmer
November 1993 **Proceedings of the 21st annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(798.76 KB) Additional Information: full citation, index terms

7 Data Security
Dorothy E. Denning, Peter J. Denning
September 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 3
Publisher: ACM Press
Full text available: pdf(1.97 MB) Additional Information: full citation, references, citings, index terms

8 Protection imperfect: the security of some computing environments
Carole B. Hogan
July 1988 **ACM SIGOPS Operating Systems Review**, Volume 22 Issue 3
Publisher: ACM Press
Full text available: pdf(1.31 MB) Additional Information: full citation, citings, index terms

9 A security architecture for fault-tolerant systems
Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

10 Computers and Privacy: A Survey
Lance J. Hoffman
June 1969 **ACM Computing Surveys (CSUR)**, Volume 1 Issue 2
Publisher: ACM Press
Full text available: pdf(1.74 MB) Additional Information: full citation, references, citings, index terms

11 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

12 On secure and pseudonymous client-relationships with multiple servers
Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press
Full text available: pdf(161.56 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper introduces a cryptographic engine, Janus, which assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. The setting is such that clients reside on a particular subnet (e.g., corporate intranet, ISP) and the servers reside anywhere on the Internet. The Janus engine allows each client-server relationship to use either weak or strong authentication on each interaction. At the same time, each interaction preserves privacy by neithe ...

Keywords: Janus function, anonymity, mailbox, persistent relationship, privacy, pseudonym

13 Protecting privacy using the decentralized label model
Andrew C. Myers, Barbara Liskov
October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 4

Publisher: ACM Press

Full text available: pdf(294.13 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Stronger protection is needed for the confidentiality and integrity of data, because programs containing untrusted code are the rule rather than the exception. Information flow control allows the enforcement of end-to-end security policies, but has been difficult to put into practice. This article describes the decentralized label model, a new label model for control of information flow in systems with mutual distrust and decentralized authority. The model improves on existing multilevel s ...

Keywords: confidentiality, declassification, downgrading, end-to-end, information flow controls, integrity, lattice, policies, principals, roles, type checking

14 Security problems in the TCP/IP protocol suite

S. M. Bellovin
April 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 2

Publisher: ACM Press

Full text available: pdf(2.72 MB) Additional Information: full citation, abstract, citings, index terms

The TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. We describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks. We also present defenses against these attacks, and conclude with a discu ...

15 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles**, Volume 33 Issue 5

Publisher: ACM Press , ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

16 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

17 Level II technical support in a distributed computing environment
Tim Leehane
September 1996 **Proceedings of the 24th annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(5.73 MB) Additional Information: full citation, references, index terms

18 Extending the Internet into the home at the Ohio State University
Fred Crowner, Art Krumsee, Sandy Li, Jerry Mantin, William B. Miller
November 1993 **Proceedings of the 21st annual ACM SIGUCCS conference on User services**
Publisher: ACM Press
Full text available: pdf(779.51 KB) Additional Information: full citation, index terms

19 A model for verification of data security in operating systems
Gerald J. Popek, David A. Farber
September 1978 **Communications of the ACM**, Volume 21 Issue 9
Publisher: ACM Press
Full text available: pdf(1.49 MB) Additional Information: full citation, abstract, references, citings, index terms

Program verification applied to kernel architectures forms a promising method for providing uncircumventably secure, shared computer systems. A precise definition of data security is developed here in terms of a general model for operating systems. This model is suitable as a basis for verifying many of those properties of an operating system which are necessary to assure reliable enforcement of security. The application of this approach to the UCLA secure operating system is also discussed ...

Keywords: operating systems, program verification, protection, security

20 Copyrights and access-rights: How DRM-based content delivery systems disrupt expectations of "personal use"
Deirdre K. Mulligan, John Han, Aaron J. Burstein
October 2003 **Proceedings of the 2003 ACM workshop on Digital rights management**
Publisher: ACM Press
Full text available: pdf(416.68 KB) Additional Information: full citation, abstract, references, index terms, review

We set out to examine whether current, DRM-based online offerings of music and movies accord with consumers' current expectations regarding the personal use of copyrighted works by studying the behavior of six music, and two film online distribution services. We find that, for the most part, the services examined do not accord with expectations of personal use. The DRM-based services studied restrict personal use in a manner inconsistent with the norms and expectations governing the purchase and ...

Keywords: access control, content distribution, copyright, digital rights management, fair use, personal use, privacy

Results 1 - 20 of 59 Result page: **1** 2 3 next

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player